

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-231173

(43) 公開日 平成9年(1997)9月5日

(51) Int.Cl. <sup>8</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 15/00	3 3 0		G 0 6 F 15/00	3 3 0 D
H 0 4 L 12/22			H 0 4 M 3/00	E
H 0 4 M 3/00			H 0 4 Q 3/545	
H 0 4 Q 3/545		9466-5K	H 0 4 L 11/26	

審査請求 未請求 請求項の数12 O L (全 18 頁)

(21) 出願番号 特願平8-33986

(22) 出願日 平成8年(1996)2月21日

(71) 出願人 000004226

日本電信電話株式会社

東京都新宿区西新宿三丁目19番2号

(72) 発明者 増井 信彦

東京都新宿区西新宿三丁目19番2号 日本

電信電話株式会社内

(74) 代理人 弁理士 伊東 忠彦

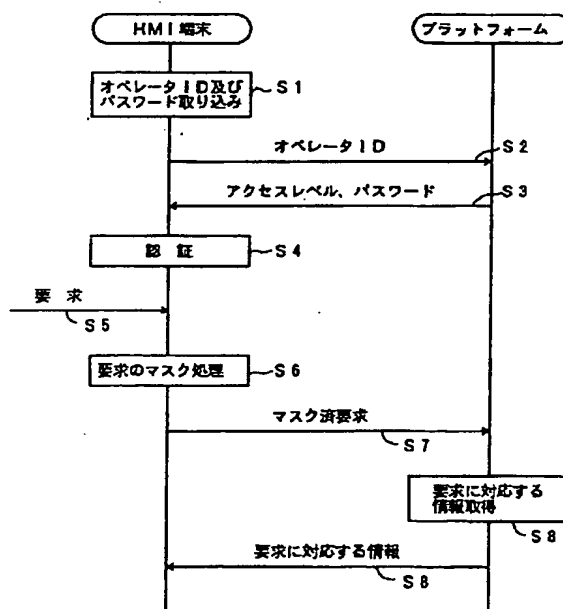
(54) 【発明の名称】 アクセスレベルによるHMI端末の利用機能のマスク方法及びシステム

(57) 【要約】

【課題】 オペレータの操作性の性能向上を図るために、オペレータのアクセスレベルに応じて利用可能なオペレーション機能の制限を各端末でマスクして行うことが可能なアクセスレベルによるHMI端末の利用機能のマスク方法及びシステムを提供する。

【解決手段】 本発明は、オペレータのアクセスレベル情報を、オペレータ毎に、プラットフォーム側に配置し、オペレータがHMI端末のオペレーション時に、アクセスレベル情報を参照して、オペレータ毎にアクセスレベル情報に基づいてHMI端末の機能のマスク処理を行う。

本発明の第1の原理を説明するための図



## 【特許請求の範囲】

【請求項1】 オペレーションシステムにおけるオペレータのアクセスレベルによるオペレーション機能を制限するためのアクセスレベルによるHMI端末の利用機能のマスク方法において、

オペレータのアクセスレベル情報を、オペレータ毎に、プラットフォーム側に配置し、

オペレータがHMI端末のオペレーション時に、前記アクセスレベル情報を参照して、オペレータ毎に前記アクセスレベル情報に基づいて前記HMI端末の機能のマスク処理を行うことを特徴とするアクセスレベルによるHMI端末の利用機能のマスク方法。

【請求項2】 オペレータから入力される要求に対して前記HMI端末の機能のマスク処理を、前記プラットフォーム側から取得したアクセスレベル情報に基づいて、前記HMI端末側で行う請求項1記載のアクセスレベルによるHMI端末の利用機能のマスク方法。

【請求項3】 オペレータがHMI端末にログインした場合に、入力されたオペレータIDとパスワードを取り込み、

前記プラットフォーム側からパスワードと前記オペレータIDに対応するアクセスレベルを取得し、

入力された前記パスワードを、前記プラットフォーム側から取得したパスワードを用いて認証し、

オペレータが前記HMI端末操作を行うことにより、要求内容を受け取り、前記アクセスレベルに基づいてマスク処理を行い、前記プラットフォーム側に転送し、

前記プラットフォーム側では、マスク処理された要求内容に対する処理を行って、その結果を前記HMI端末に転送する請求項2記載のアクセスレベルによるHMI端末の利用機能のマスク方法。

【請求項4】 オペレータから入力される要求に対して前記HMI端末の機能のマスク処理を、前記プラットフォーム側に保持されているアクセスレベル情報に基づいて、前記プラットフォーム側で行う請求項1記載のアクセスレベルによるHMI端末の利用機能のマスク方法。

【請求項5】 オペレータがHMI端末にログインした場合に、入力されたオペレータIDとパスワードを取り込み、

前記プラットフォーム側からパスワードと前記オペレータIDに対応するアクセスレベルを取得し、

入力された前記パスワードを、前記プラットフォーム側から取得したパスワードを用いて認証し、アクセスレベルを判定し、前記オペレータIDと前記アクセスレベルを前記プラットフォームに転送し、

オペレータが前記HMI端末操作を行うことにより、要求内容を受け取り、前記プラットフォームに転送し、

前記プラットフォーム側において、前記要求内容に対して前記アクセスレベルに応じたマスク処理を行い、

前記マスクをかけた要求内容に対する処理を行い、その

結果を前記HMI端末に転送する請求項4記載のアクセスレベルによるHMI端末の利用機能のマスク方法。

【請求項6】 前記要求内容が書き込み要求である場合には、オペレータID及び該書き込み要求に関する履歴情報を保持する請求項3または5記載のアクセスレベルによるHMI端末の利用機能のマスク方法。

【請求項7】 オペレーションシステムにおけるオペレータのアクセスレベルによるオペレーション機能を制限するためのアクセスレベルによるHMI端末の利用機能のマスクシステムであって、

オペレータのアクセスレベル情報を、オペレータ毎に保持するプラットフォームと、

オペレータからのHMI端末のオペレーション時に、前記アクセスレベル情報を参照して、オペレータ毎の前記アクセスレベル情報に基づいて前記HMI端末の機能のマスク処理を行うHMI端末とを有することを特徴とするアクセスレベルによるHMI端末の利用機能のマスクシステム。

【請求項8】 前記HMI端末は、

オペレータがHMI端末にログインした場合に、入力されたオペレータIDとパスワードを取得するオペレータID取得手段と、

入力されたパスワードと前記プラットフォーム側で管理されるパスワードを用いて、前記オペレータIDの認証を行う認証手段と、

前記プラットフォーム側より取得したアクセスレベル情報に基づいて前記オペレータのアクセスレベルを決定するアクセスレベル判定手段と、

前記オペレータからの要求について前記アクセスレベル判定手段により決定されたアクセスレベルに応じて該要求をマスクするマスク手段と、

前記マスク手段によりマスク処理された要求を前記プラットフォーム側に転送し、該プラットフォーム側から取得した要求に対応する情報を取得し、前記オペレータに提示する情報提示手段とを有し、

前記プラットフォームは、

オペレータ毎のアクセスレベル情報を保持するアクセスレベル保持手段と、

前記HMI端末から取得した前記マスク処理された要求に基づいて該要求に対応する処理を行い、その結果を前記HMI端末に提供する情報提供手段とを有する請求項7記載のアクセスレベルによるHMI端末の利用機能のマスクシステム。

【請求項9】 前記プラットフォームは、前記HMI端末からの要求に対応するデータを提供するためのデータ及び、前記要求が書き込み要求である場合に、オペレータID及び書き込み要求に関する履歴情報を保持するデータ保持手段を含む請求項8記載のデータ保持手段を有する。

【請求項10】 オペレーションシステムにおけるオペ

レータのアクセスレベルによるオペレーション機能を制限するためのアクセスレベルによるHMI端末の利用機能のマスクシステムであって、オペレータのアクセスレベル情報をオペレータ毎に保持し、該アクセスレベル情報に基づいて前記HMI端末からの要求に対して前記HMI端末の機能のマスク処理を行うプラットフォームと、オペレータID、パスワードの認証を行い、オペレータからの要求を前記プラットフォームに転送し、該プラットフォームから要求に対応する情報を取得するHMI端末とを有することを特徴とするアクセスレベルによるHMI端末の利用機能のマスクシステム。

【請求項11】 前記HMI端末は、オペレータがHMI端末にログインした場合に、入力されたオペレータIDとパスワードを取得するオペレータID取得手段と、入力されたパスワードと前記プラットフォーム側で管理されるパスワードを用いて、前記オペレータIDの認証を行う認証手段と、前記プラットフォーム側より取得したアクセスレベル情報に基づいて前記オペレータのアクセスレベルを決定するアクセスレベル判定手段と、前記オペレータからの要求を前記プラットフォーム側に送信し、前記プラットフォームから該要求に対応する情報を取得して、該オペレータに提示する情報提示手段とを有し、前記プラットフォームは、オペレータ毎のアクセスレベルを保持するアクセスレベル保持手段と、前記HMI端末から前記要求を取得する要求取得手段と、前記HMI端末の前記アクセスレベル判定手段により決定されたアクセスレベルに応じて前記要求取得手段で取得した該要求をマスクするマスク手段と、前記マスク手段によりマスク処理された要求に対応する処理を行い、その結果を前記HMI端末に提供する情報提供手段とを有する請求項10記載のアクセスレベルによるHMI端末の利用機能のマスクシステム。

【請求項12】 前記プラットフォームは、前記HMI端末からの要求に対応するデータを提供するためのデータ及び、前記要求が書き込み要求である場合に、オペレータID及び書き込み要求に関する履歴情報を保持するデータ保持手段を有する請求項11記載のアクセスレベルによるHMI端末の利用機能のマスクシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、アクセスレベルによるHMI端末の利用機能のマスク方法及びシステムに係り、特に、オペレーションシステム（以下Opsと記す）における、オペレータのアクセスレベルによるオペ

レーション機能の制限に必要なアクセスレベルによるHMI端末の利用機能のマスク方法及びシステムに関する。

【0002】詳しくは、Opsは、通常、複数の場所に設置されている複数のHMI端末から複数のオペレータによって利用される。そのため、実際にHMI端末を操作するオペレータのアクセスレベルに応じて、利用できるオペレーション機能の制限を各端末毎にマスクして行うことが重要である。

【0003】また、そのため、セキュリティを考慮した上で、オペレータを自動認証が可能なアクセスレベルによるHMI端末の利用機能のマスク方法及びシステムが望まれている。

【0004】

【従来の技術】従来、オペレータのアクセスレベルに応じて利用できるオペレーション機能を制限するためには、各端末毎に異なるオペレーション用のプログラムを配付しておいて、使用する端末でアクセスレベルを区別したり、オペレータが自分で利用する機能を特定して利用する等の方法を運用対処策としている。

【0005】

【発明が解決しようとする課題】しかしながら、上記従来のシステムでは、以下のような問題がある。

(1) 機能を制限するためのマスクの設定単位が、オペレータ毎に割り付けるのか、又は、端末毎に割り付けるのかが明確でない。

【0006】(2) システム上でオペレータのアクセスレベル情報を保持する箇所を決めるために、メンテナンス、セキュリティの観点を考慮していない。

本発明は、上記の点に鑑みなされたもので、上記従来の問題点を解決し、オペレータの操作性の性能向上を図るために、オペレータのアクセスレベルに応じて利用可能なオペレーション機能の制限を各端末でマスクして行うことが可能なアクセスレベルによるHMI端末の利用機能のマスク方法及びシステムを提供することを目的とする。

【0007】

【課題を解決するための手段】第1の発明は、オペレーションシステムにおけるオペレータのアクセスレベルによるオペレーション機能を制限するためのアクセスレベルによるHMI端末の利用機能のマスク方法において、オペレータのアクセスレベル情報を、オペレータ毎に、プラットフォーム側に配置し、オペレータがHMI端末のオペレーション時に、アクセスレベル情報を参照して、オペレータ毎にアクセスレベル情報に基づいてHMI端末の機能のマスク処理を行う。

【0008】第2の発明は、オペレータから入力される要求に対してHMI端末の機能のマスク処理を、プラットフォーム側から取得したアクセスレベル情報に基づいて、HMI端末側で行う。図1は、本発明の第1の原理

を説明するための図である。

【0009】第3の発明は、オペレータがHMI端末にログインした場合に、入力されたオペレータIDとパスワードを取り込み（ステップ1）、オペレータIDをプラットフォーム側に転送し（ステップ2）、プラットフォーム側からパスワードとオペレータIDに対応するアクセスレベルを取得し（ステップ3）、入力されたパスワードを、プラットフォーム側から取得したパスワードを用いて認証し（ステップ4）、オペレータがHMI端末操作を行うことにより、要求内容を受け取り（ステップ5）、アクセスレベルに基づいてマスク処理を行い（ステップ6）、プラットフォーム側に転送し（ステップ7）、プラットフォーム側では、マスク処理された要求内容に対する処理を行って（ステップ8）、その結果をHMI端末に転送する（ステップ9）。

【0010】第4の発明は、オペレータから入力される要求に対してHMI端末の機能のマスク処理を、プラットフォーム側に保持されているアクセスレベル情報に基づいて、プラットフォーム側で行う。図2は、本発明の第2の原理を説明するための図である。

【0011】第5の発明は、オペレータがHMI端末にログインした場合に、入力されたオペレータIDとパスワードを取り込み（ステップ10）、オペレータIDをプラットフォーム側に転送し（ステップ11）、プラットフォーム側からパスワードとオペレータIDに対応するアクセスレベルを取得し（ステップ12）、入力されたパスワードを、プラットフォーム側から取得したパスワードを用いて認証し（ステップ13）、アクセスレベルを判定し、オペレータIDとアクセスレベルをプラットフォームに転送し（ステップ14）、オペレータがHMI端末操作を行うことにより、要求内容を受け取り、プラットフォームに転送し（ステップ15）、プラットフォーム側において、要求内容に対してアクセスレベルに応じたマスク処理を行い（ステップ16）、マスクをかけた要求内容に対する処理を行って（ステップ17）、その結果をHMI端末に転送する（ステップ18）。

【0012】第6の発明は、要求内容が書込み要求である場合には、オペレータID及び該書込み要求に関する履歴情報を保持する。第7の発明は、オペレーションシステムにおけるオペレータのアクセスレベルによるオペレーション機能を制限するためのアクセスレベルによるHMI端末の利用機能のマスクシステムであって、オペレータのアクセスレベル情報を、オペレータ毎に保持するプラットフォームと、オペレータからのHMI端末のオペレーション時に、アクセスレベル情報を参照して、オペレータ毎のアクセスレベル情報に基づいてHMI端末の機能のマスク処理を行うHMI端末とを有する。

【0013】図3は、本発明の第1の原理構成図である。第8の発明において、HMI端末10は、オペレー

タがHMI端末10にログインした場合に、入力されたオペレータIDとパスワードを取得するオペレータID取得手段11と、入力されたパスワードとプラットフォーム側で管理されるパスワードを用いて、オペレータIDの認証を行う認証手段12と、プラットフォーム側より取得したアクセスレベル情報に基づいてオペレータのアクセスレベルを決定するアクセスレベル判定手段13と、オペレータからの要求についてアクセスレベル判定手段13により決定されたアクセスレベルに応じて該要求をマスクするマスク手段14と、マスク手段によりマスク処理された要求をプラットフォーム側に転送し、該プラットフォーム側から取得した要求に対応する情報を取得し、オペレータに提示する情報提示手段15とを有し、プラットフォーム20は、オペレータ毎のアクセスレベル情報を保持するアクセスレベル保持手段21と、HMI端末10から取得したマスク処理された要求に基づいて該要求に対応する処理を行って、その結果をHMI端末10に提供する情報提供手段22とを有する。

【0014】第9の発明は、第8の発明において、プラットフォーム20が、HMI端末10からの要求に対応するデータを提供するためのデータ及び、要求が書込み要求である場合に、オペレータID及び書込み要求に関する履歴情報を保持するデータ保持手段を含む。

【0015】第10の発明は、オペレーションシステムにおけるオペレータのアクセスレベルによるオペレーション機能を制限するためのアクセスレベルによるHMI端末10の利用機能のマスクシステムであって、オペレータのアクセスレベル情報をオペレータ毎に保持し、該アクセスレベル情報に基づいてHMI端末10からの要求に対してHMI端末10の機能のマスク処理を行うプラットフォームと、オペレータID、パスワードの認証を行い、オペレータからの要求をプラットフォームに転送し、該プラットフォーム側から要求に対応する情報を取得するHMI端末10とを有する。

【0016】図4は、本発明の第2の原理構成図である。第11の発明において、HMI端末10は、オペレータがHMI端末10にログインした場合に、入力されたオペレータIDとパスワードを取得するオペレータID取得手段11と、入力されたパスワードとプラットフォーム側で管理されるパスワードを用いて、オペレータIDの認証を行う認証手段12と、プラットフォーム20側より取得したアクセスレベル情報に基づいてオペレータのアクセスレベルを決定するアクセスレベル判定手段13と、オペレータからの要求をプラットフォーム側に送信し、プラットフォーム側から該要求に対応する情報を取得して、該オペレータに提示する情報提示手段15とを有し、プラットフォーム20は、オペレータ毎のアクセスレベルを保持するアクセスレベル保持手段21と、HMI端末10から要求を取得する要求取得手段23と、HMI端末10のアクセスレベル判定手段により

決定されたアクセスレベルに応じて要求取得手段で取得した該要求をマスクするマスク手段24と、マスク手段24によりマスク処理された要求に対応する処理を行って、その結果をHMI端末10に提供する情報提供手段22とを有する。

【0017】第12の発明は、プラットフォーム20が、HMI端末からの要求に対応するデータを提供するためのデータ及び、要求が書き込み要求である場合に、オペレータID及び書き込み要求に関する履歴情報を保持するデータ保持手段を含む。このように、本発明は、アクセスレベルの設定単位を、HMI端末毎に割り付けるのではなく、オペレータごとに自動的に割り付けるものである。即ち、利用できる機能をオペレータ毎に設定できるようにするものである。従って、従来のように、各端末毎に異なるオペレーション用のプログラムを配付しておく必要はない。

【0018】また、オペレータのアクセスレベル情報は、HMI端末10側ではなく、プラットフォーム(PF)側に保持するようにすることにより、メンテナンス性の見地からHMI端末10でオペレータのアクセスレベル情報を保持した場合には、オペレータのアクセスレベル情報をデリバリする際に、全てのHMI端末に対して設定を行う必要があるが、PF側においてオペレータのアクセスレベル情報を保持することにより、全HMI端末側のオペレータのアクセスレベル情報をPH側で一元管理することができる。また、セキュリティ性の見地からは、オペレータのアクセスレベル情報は、各HMI端末に置かず済むため、PFのデータベースのセキュリティ機構を利用することができるため、HMI端末を扱うオペレータがアクセスレベル情報を操作することは不可能であり、秘匿性を有することが可能である。

【0019】上記のように、本発明は、オペレータ単位にアクセスレベルに応じたオペレーション機能をマスクすることができると共に、オペレータのアクセスレベル情報をメンテナンス性及びセキュリティ性を考慮して管理することが可能となる。

【0020】

【発明の実施の形態】図5は、本発明の第1のアクセスレベルによるHMI端末の利用機能のマスクシステムの構成を示す。以下に示す第1の方法は、第1のマスク処理をHMI端末において行うものである。

【0021】同図に示すシステムは、複数台のHMI端末100、～100、と1つの共通PF/DB200から構成される。各HMI端末100は、オペレータID入力部101、アクセスレベル判定部102、要求入力/結果出力部104、マスク処理部105から構成される。

【0022】オペレータID入力部101は、オペレータがHMI端末のログインする等の利用開始するための検証時に、入力されたオペレータIDとパスワードを取

込み、そのオペレータIDとパスワードをアクセスレベル判定部102に転送する。アクセスレベル判定部102は、オペレータID入力部101から転送されたオペレータIDを受け取って保持しておき、オペレータIDを共通PF/DB200に転送する。また、共通PF/DB200からパスワードとアクセスレベルを受け取ると、当該パスワードを共通PF/DB200から送られたパスワードとを用いて認証を行い、正しく認証できた場合には、オペレータIDとアクセスレベルをマスク処理部105に転送する。

【0023】マスク処理部105は、アクセスレベル判定部102から転送されたオペレータIDとアクセスレベルを受け取り、保持しておき、HMI端末100自体からの要求を、要求受け取り/返却部104を介して受け取ると、アクセスレベルに応じて要求内容にマスクをかけ、マスクをかけた要求内容を、共通PF/DB200に転送する。

【0024】要求受け取り/返却部104は、オペレータがHMI端末100からの要求を受け取り、また、マスク処理部105から送られた要求内容の情報を受け取りHMI端末100に要求内容の情報を表示する。共通PF/DB200は、オペレータ管理テーブル201、要求算出部202、データ保持部203を有する。

【0025】オペレータ管理テーブル201は、HMI端末100のアクセスレベル判定部102から転送されたオペレータIDを受け取り、保持しているオペレータ管理情報の中から、該当するオペレータIDのパスワードとアクセスレベルを抽出し、そのパスワードとアクセスレベルをHMI端末100のアクセスレベル判定部102に転送する。オペレータ管理テーブル201において、オペレータ管理情報は、図6に示すように保持している。オペレータ管理情報は、オペレータID、パスワード及びアクセスレベル等である。

【0026】要求算出部202は、HMI端末100のマスク処理部105からの要求内容を受け取り、当該要求内容に相当する情報をデータ保持部203に転送すると共に、データ保持部203から当該要求内容に該当する取得して、HMI端末のマスク処理部105に転送するデータ保持部203は、要求算出部202から要求された情報を要求算出部202に転送する。要求内容が情報の書き込みの場合は、オペレータIDを含めた変更履歴を作成し、データを書き込みする。

【0027】図7は、本発明の第1のアクセスレベルによるHMI端末の利用機能のマスクシステムの動作を示すシーケンスチャートである。

ステップ101) オペレータID入力部101は、オペレータがHMI端末100にログインする等の利用開始操作を行うと、当該オペレータから入力されるオペレータID及びパスワードを取得する。

【0028】ステップ102) アクセスレベル判定部

102は、オペレータID入力部101から取得したオペレータID(H)とパスワード(H)をワークメモリに保持する。

ステップ103) アクセスレベル判定部102は、オペレータ毎のアクセスレベルを判定するために、共通PF/DB200のオペレータ管理テーブル201に対してオペレータID(H)を転送する。

【0029】ステップ104) オペレータ管理テーブル201において、アクセスレベル判定部102から取得したオペレータID(H)をキーにして、当該オペレータのアクセスレベルを抽出する。

ステップ105) オペレータ管理テーブル201が、パスワード(P)と抽出されたアクセスレベルをHMI端末100のアクセスレベル判定部102に転送する。

【0030】ステップ106) HMI端末100のアクセスレベル判定部102は、ワークメモリ内に保持しているパスワード(H)と、共通PF/DB200から取得したパスワード(P)を用いて認証を行い、正しいと認証できた場合には、オペレータIDとアクセスレベルをマスク処理部105に転送する。

【0031】ステップ107) ここで、HMI端末100のオペレータから要求が入力されると、要求入力/結果出力部104は、当該要求を取得し、当該要求をマスク処理部105に転送する。これにより、マスク処理部105は、当該要求内容にマスク処理を行う。

【0032】ステップ108) マスク処理部105は、マスクをかけた要求内容を共通PF/DB200の要求算出部202に転送する。

ステップ109) 要求算出部202は、マスク処理部105から取得した要求内容を取得し、要求内容に相当する情報をデータ保持部203に要求する。これによりデータ保持部203は、当該要求に対応する情報を抽出して、要求算出部202に返却する。

【0033】ステップ110) 要求算出部202は、データ保持部203からの情報を取得し、要求内容の情報を算出して、マスク処理部105に転送する。

ステップ111) マスク処理部105は、要求算出部202から取得した要求内容の情報を受け取り、要求内容の情報を要求入力/結果出力部104に転送する。これにより、要求入力/結果出力部104は、HMI端末100に当該要求内容の情報を表示する。

【0034】このように、上記の第1のシステムでは、HMI端末100内のアプリケーションのレベルでマスク処理を行うため、情報取得のオブジェクトライブラリ群にその仕組みを持たせ、比較的簡単にマスクを実施することができる。図8は、本発明の第2のアクセスレベルによるHMI端末の利用機能のマスクシステムの構成を示す。以下に示す第2のシステムは、マスク処理を共通PF/DB側において行うものである。

【0035】同図に示すシステムは、オペレータID入

力部101、アクセスレベル判定部102、要求解析部103及び要求入力/結果出力部104より構成されるHMI端末100と、オペレータ管理テーブル201、データ保持部203、及び要求・マスク処理部204より構成される。

【0036】HMI端末100のオペレータID入力部101は、オペレータがHMI端末のログインする等の利用開始するための検証時に、入力されたオペレータIDとパスワードを取込み、そのオペレータIDとパスワードをアクセスレベル判定部102に転送する。

【0037】アクセスレベル判定部102は、オペレータID入力部101から転送されたオペレータIDとパスワードを受け取り、パスワードは保持し、オペレータIDを共通PF/DB200に転送する。また、共通PF/DB200からパスワードとアクセスレベルを受け取ると、当該パスワードを共通PF/DB200から送られたパスワードとを用いて認証を行い、正しく認証できた場合には、オペレータIDとアクセスレベルを共通PF/DB200に転送する。

【0038】要求入力/結果出力部104は、オペレータがHMI端末で要求を行った時に、当該要求を受け取って要求解析部103に転送する。また、要求解析部103を介して、共通PF/DB200からの要求に対応する情報を取得すると、当該情報をオペレータに提示する。

【0039】要求解析部103は、要求入力/結果出力部104から取得した要求を共通PF/DB200に転送する。また、共通PF/DB200から取得した要求に対応する情報を要求入力/結果出力部104に転送する。共通PF/DB200は、オペレータ管理テーブル201、データ保持部203及び、要求・マスク処理部204より構成される。

【0040】オペレータ管理テーブル201及びデータ保持部203は、前述の図5の構成と同様である。要求・マスク処理部204は、HMI端末100から取得したオペレータIDとアクセスレベルを受け取って保持しておき、HMI端末100の要求解析部103から、オペレータの要求を受け取り、当該オペレータのアクセスレベルに応じて要求内容にマスクをかけた要求内容に相当する情報をデータ保持部203に要求する。

【0041】次に、第2のアクセスレベルによるHMI端末の利用機能のマスクシステムの動作を示す。図9は、本発明の第2のアクセスレベルによるHMI端末の利用機能のマスクシステムの動作を示すシーケンスチャートである。

【0042】ステップ201) オペレータID入力部101は、オペレータがHMI端末100にログインする等の利用開始操作を行うと、当該オペレータから入力されるオペレータID及びパスワードを取得する。

ステップ202) アクセスレベル判定部102は、オ

オペレータID入力部101から取得したオペレータID (H)とパスワード(H)をワークメモリに保持する。

【0043】ステップ203) アクセスレベル判定部102は、オペレータ毎のアクセスレベルを判定するために、共通PF/DB200のオペレータ管理テーブル201に対してオペレータID(H)を転送する。

ステップ204) オペレータ管理テーブル201において、アクセスレベル判定部102から取得したオペレータIDをキーにして、当該オペレータのアクセスレベルを抽出する。

【0044】ステップ205) オペレータ管理テーブル201は、パスワード(P)と抽出されたアクセスレベルをHMI端末100のアクセスレベル判定部102に転送する。

ステップ206) HMI端末100のアクセスレベル判定部102は、ワークメモリ内に保持しているパスワード(H)と、共通PF/DB200から取得したパスワード(P)を用いて認証を行う。

【0045】ステップ207) 認証において、正しいと認証できた場合には、オペレータIDとアクセスレベルを、共通PF/DB200の要求・マスク処理部204に転送する。

ステップ208) 共通PF/DB200の要求・マスク処理部204は、取得したオペレータIDとアクセスレベルを保持しておく。

【0046】ステップ209) ここで、オペレータから要求が入力されると、HMI端末100の要求入力/結果出力部104は、当該要求内容を共通PF/DB200の要求・マスク処理部204に転送する。

ステップ210) 共通PF/DB200の要求・マスク処理部204は、要求内容にマスク処理を行い、データ保持部203にマスク処理済の要求を発行する。

【0047】ステップ211) 要求・マスク処理部204は、データ保持部203から当該要求に対応するデータを取得して、HMI端末100の要求解析部103に転送する。

ステップ212) HMI端末100の要求解析部103は、取得したデータを要求入力・結果出力部104に転送する。これにより、要求入力・結果出力部104は、HMI端末100に当該要求内容の情報を表示する。

【0048】このように、第2のアクセスレベルによるHMI端末の利用機能のマスクシステムでは、要求内容にマスクをかける箇所は共通PF/DB200側で行う。第2のアクセスレベルによるHMI端末の利用機能のマスクシステムでは、共通PF/DB200側において、アプリケーションレベルでマスク処理を行うため、メンテナンスの際に当該共通PF/DB200側で一元管理を行うことが可能であるため、各HMI端末100にデリバリする必要がない。これは、オブジェクト管理

アプリケーションをHMI情報取得窓口として、共通PF/DB200に構築し、オペレータのアクセスレベル情報に従って、HMI端末100に返却する情報を制御するからである。

【0049】

【実施例】以下に、本発明の実施例を図面と共に説明する。

《第1の実施例》本実施例を前述の図7のシーケンスチャートに基づいて説明する。

10 【0050】まず、本実施例では、オペレータのアクセスレベルを図6に示すように「特権」、「一般」、「デモ」の3つのレベルとする。HMI端末100のオペレータIDを“23456789”とし、パスワードを“BY3CCZ4F”とする。共通PF/DB200のオペレータ管理テーブル201には、図6に示す内容が予め登録されているものとする。

【0051】(1) オペレータID入力部101は、オペレータからオペレータIDとして、“23456789”とパスワード“BY3CCZ4F”が入力される

20 (ステップ101)。(2) アクセスレベル判定部102は、オペレータID入力部101から取得したオペレータID“23456789”とパスワード“BY3CCZ4F”をワークメモリに保持する(ステップ102)。

【0052】(3) アクセスレベル判定部102は、共通PF/DB200のオペレータ管理テーブル201に対してオペレータID(23456789)を転送する(ステップ103)。

(4) オペレータ管理テーブル201において、アクセスレベル判定部102から取得したオペレータID(23456789)をキーにして、アクセスレベル「一般用」を取得する(ステップ104)。

【0053】(5) 共通PF/DB200は、アクセスレベル「一般用」とパスワード“BY3CCZ4F”をHMI端末100のアクセスレベル判定部102に転送する。

(6) アクセスレベル判定部102は、ワークメモリ内に格納されているパスワード(BY3CCZ4F)と、共通PF/DB200から取得したパスワード“BY3CCZ4F”とを比較する。この例では、同一であるために正しいと認証する。このオペレータID(23456789)とパスワード(BY3CCZ4F)をマスク処理部105に転送する(ステップ106)。

【0054】(7) HMI端末100のオペレータから、

「実際の苦情の全リストの一覧」

という要求が入力されると、要求入力/結果出力部104は、当該要求を取得して、当該要求のマスク処理を行う。マスク処理は、図6に示すように、当該オペレータのアクセスレベルは「一般」であるので、マスク処理

は、図10に示すように「オペレータの担当する苦情のリスト一覧」となり、当該オペレータが担当する範囲に限定される(ステップ107)。

【0055】(8) マスク処理部105は、マスクをかけた要求内容「オペレータの担当する苦情のリスト一覧」を共通PF/DB200の要求算出部202に転送する(ステップ108)。

(9) 要求算出部202は、データ保持部203から当該要求に対応するリスト一覧のデータを抽出して、要求算出部202に返却する(ステップ109)。

【0056】(10) 要求算出部202は、リスト一覧のデータを取得して、マスク処理部105に転送する(ステップ110)。

(11) マスク処理部105は、要求内容に対応するデータ(リスト一覧)を受け取り、要求入力/結果出力部104に転送する(ステップ111)。

【0057】(12) これにより、要求入力/結果出力部104は、ディスプレイ等の出力機器に当該リストを出力する。

このように、本実施例では、HMI端末100側においてマスク処理された要求内容に対応するデータが共通PF/DB200側より取得することができる。

【0058】なお、上記の実施例では、オペレータのアクセスレベルが「一般」の例を説明したが、図10の例においては、オペレータのアクセスレベルが「特権」の場合には、マスク処理は行わず、実際の苦情の全リストの一覧の提供が要求内容となる。また、「デモ」の場合には、デモ用の苦情リストの一覧の提供が要求内容となる。

【0059】《第2の実施例》次に、前述の図9のシーケンスチャートに従って、本発明の第2の実施例を説明する。本実施例では、オペレータのアクセスレベルを「特権」、「一般」、「デモ」の3つのレベルとする。

【0060】HMI端末100のオペレータIDを“34567890”とし、パスワードを“CZ4DDA5E”とする。共通PF/DB200のオペレータ管理テーブル201には、図6に示す内容が予め登録されているものとする。

(1) オペレータID入力部101は、当該オペレータから入力されるオペレータID及びパスワードを取得する(ステップ201)。

【0061】(2) アクセスレベル判定部102は、オペレータID入力部101から取得したオペレータID(34567890)とパスワード(CZ4DDA5E)をワークメモリに保持する(ステップ202)。

(3) アクセスレベル判定部102は、オペレータ毎のアクセスレベルを判定するために、共通PF/DB200のオペレータ管理テーブル201に対してオペレータID(34567890)を転送する(ステップ203)。

【0062】(4) オペレータ管理テーブル201において、アクセスレベル判定部102から取得したオペレータID(34567890)によりオペレータのアクセスレベル「デモ」を抽出する(ステップ204)。

(5) オペレータ管理テーブル201は、パスワード(CZ4DDA5E)と抽出されたアクセスレベル(デモ)をHMI端末100のアクセスレベル判定部102に転送する(ステップ205)。

【0063】(6) HMI端末100のアクセスレベル判定部102は、ワークメモリ内に保持しているパスワード(CZ4DDA5E)と、共通PF/DB200から取得したパスワード(CZ4DDA5E)を用いて認証を行う。

(7) この認証では、双方のパスワードが一致するため、正しいと認証する。従って、オペレータID(34567890)とアクセスレベル(デモ)を、共通PF/DB200の要求・マスク処理部204に転送する(ステップ207)。

【0064】(8) 共通PF/DB200の要求・マスク処理部204は、取得したオペレータID(34567890)とアクセスレベル(デモ)をワークメモリ内に保持しておく(ステップ208)。

(9) ここで、オペレータから以下のような要求が入力されると、

「実際の全顧客の契約条件の一覧」

HMI端末100の要求入力/結果出力部104は、当該要求内容を共通PF/DB200の要求・マスク処理部204に転送する(ステップ209)。

【0065】(10) 共通PF/DB200の要求・マスク処理部204は、図11に示すように、要求内容にマスク処理を行い、データ保持部203に以下のようなマスク処理済の要求を発行する(ステップ210)。

【0066】「デモ用の顧客の契約条件の一覧」

(11) 要求・マスク処理部204は、データ保持部203から当該要求「デモ用の顧客の契約条件の一覧」に対応するデータを取得して、HMI端末100の要求解析部103に転送する(ステップ211)。

【0067】(12) HMI端末100の要求解析部103は、取得したデータを要求入力・結果出力部104に転送する。これにより、要求入力・結果出力部104は、HMI端末100に当該要求内容の情報を表示する。なお、上記の実施例では、オペレータのアクセスレベルが「デモ」の例を説明したが、オペレータのアクセスレベルが「特権」の場合には、マスク処理は行わず、実際の全顧客の契約条件の一覧の提供が要求内容となる。また、「一般」の場合には、オペレータの所属する部署の担当する顧客の契約条件の一覧の提供が要求内容となる。

【0068】《第3の実施例》次に、第3の実施例として、要求内容が書き込み要求の場合の例を説明する。具



体的な要求内容を「全ての解約者の情報を消去する」として説明する。この場合におけるアクセスレベルを「一般」とし、HMI端末100のオペレータIDを“23456789”とし、パスワードを“BY3CCZ4D”とする。共通PF/DB200のオペレータ管理テーブル201には、図6に示す内容が予め登録されているものとする。

【0069】マスク処理は、上記の第2の実施例に沿って行うものとする。つまり、マスク処理を共通PF/DB200側で行う。従って、前述の図9に示すシーケンスチャートに沿って説明する。

(1) オペレータID入力部101は、当該オペレータから入力されるオペレータID(23456789)及びパスワード(BY3CCZ4D)を取得する(ステップ201)。

【0070】(2) アクセスレベル判定部102は、オペレータID入力部101から取得したオペレータID(23456789)とパスワード(BY3CCZ4D)をワークメモリに保持する(ステップ202)。

(3) アクセスレベル判定部102は、オペレータ毎のアクセスレベルを判定するために、共通PF/DB200のオペレータ管理テーブル201に対してオペレータID(23456789)を転送する(ステップ203)。

【0071】(4) 図6に示すオペレータ管理テーブル201において、アクセスレベル判定部102から取得したオペレータID(23456789)をキーにして、当該オペレータのアクセスレベル「一般」を抽出する(ステップ204)。

(5) オペレータ管理テーブル201は、パスワード(BY3CCZ4D)と抽出されたアクセスレベル(一般)をHMI端末100のアクセスレベル判定部102に転送する(ステップ205)。

【0072】(6) HMI端末100のアクセスレベル判定部102は、ワークメモリ内に保持しているパスワード(BY3CCZ4D)と、共通PF/DB200から取得したパスワード(BY3CCZ4D)を用いて認証を行う。

(7) この認証では、双方のパスワードが一致するため、正しいと認証する。従って、オペレータID(23456789)とアクセスレベル(一般)を、共通PF/DB200の要求・マスク処理部204に転送する(ステップ207)。

【0073】(8) 共通PF/DB200の要求・マスク処理部204は、取得したオペレータID(23456789)とアクセスレベル(一般)をワークメモリ内に保持しておく(ステップ208)。

(9) ここで、オペレータから以下のような要求が入力されると、

「全ての解約者の情報を消去する」

HMI端末100の要求入力/結果出力部104は、当該要求内容を共通PF/DB200の要求・マスク処理部204に転送する(ステップ209)。

【0074】(10) 共通PF/DB200の要求・マスク処理部204は、図12に示すように、要求内容にマスク処理を行い、データ保持部203に以下のようなマスク処理済の要求を発行する(ステップ210)。「オペレータが担当した解約者の情報のみを消去する」このとき、要求・マスク処理部204は、データ保持部203に変更履歴用の領域を用意し、当該領域に当該オペレータのオペレータID(23456789)と当該処理日時及び解約者情報を書き込む。

【0075】(11) 要求・マスク処理部204は、データ保持部203が保持する契約者ファイルに対して、当該要求「オペレータが担当した解約者の情報のみを消去する」に対応する更新処理を行い、更新結果をHMI端末100の要求解析部103に転送する(ステップ211)。

【0076】(12) HMI端末100の要求解析部103は、更新結果を要求入力・結果出力部104に転送する。これにより、要求入力・結果出力部104は、HMI端末100に当該更新結果を表示する。

このように、要求内容が情報を参照する場合には、上記の(10)の後半の処理は不要であるが、情報を投入/修正/削除等の更新処理を行う書き込み要求を行う場合には、変更者であるオペレータの情報及び変更記録情報を変更履歴として保持可能なように、マスクをかけた要求内容に相当する情報をデータ保持部203に格納する処理を行う。

【0077】上記の第3の実施例では、前述の第2の実施例に沿って説明したが、第1の実施例のように、HMI端末100側でマスク処理を行う場合には、HMI端末100のマスク処理部105でマスク処理された要求に応じて、書き込み要求がある場合には、共通PF/DB200の要求算出部202においてデータ保持部203に変更情報を格納する処理を行う。

【0078】上述のように、上記の各実施例によれば、HMI端末100において、オペレータのアクセスレベルに応じて、利用できるオペレーション機能をマスクすることができる。また、オペレータのアクセスレベル情報は共通PF/DB200で管理しているので、不用意にアクセスされることがないように制御できる。

【0079】なお、本発明は、上記の実施例に限定されことなく、特許請求の範囲内で種々変更・応用が可能である。

【0080】

【発明の効果】上述のように、本発明によれば、オペレータのアクセスレベルに応じて利用できるオペレーション機能の制限を各HMI端末でマスクして行うことができる。また、メンテナンス、セキュリティを考慮したオ

ベレータのアクセスレベル情報の管理を行うことができる。

【図面の簡単な説明】

【図1】本発明の第1の原理を説明するための図である。

【図2】本発明の第2の原理を説明するための図である。

【図3】本発明の第1の原理構成図である。

【図4】本発明の第2の原理構成図である。

【図5】本発明の第1のアクセスレベルによるHMI端末の利用機能のマスクシステムの構成図である。

【図6】本発明のオペレータ管理テーブルの構成例を示す図である。

【図7】本発明の第1のアクセスレベルによるHMI端末の利用機能のマスクシステムの動作を示すシーケンスチャートである。

【図8】本発明の第2のアクセスレベルによるHMI端末の利用機能のマスクシステムの構成図である。

【図9】本発明の第2のアクセスレベルによるHMI端末の利用機能のマスクシステムの動作を示すシーケンスチャートである。

【図10】本発明の第1の実施例のアクセスレベルとマスクをかけた要求内容の例を示す図である。

【図11】本発明の第2の実施例のアクセスレベルとマスクをかけた要求内容の例を示す図である。

\*【図12】本発明の第3の実施例のアクセスレベルとマスクをかけた要求内容の例を示す図である。

【符号の説明】

- 10 HMI端末
- 11 オペレータID取得手段
- 12 認証手段
- 13 アクセスレベル判定手段
- 14 マスク手段
- 15 情報提示手段
- 20 プラットフォーム
- 21 アクセスレベル保持手段
- 22 情報提供手段
- 23 要求取得手段
- 24 マスク手段
- 100 HMI端末
- 101 オペレータID入力部
- 102 アクセスレベル判定部
- 103 要求解析部
- 104 要求入力/結果出力部
- 105 マスク処理部
- 200 共通PF/DB
- 201 オペレータ管理テーブル
- 202 要求算出部
- 203 データ保持部
- 204 要求・マスク処理部

【図6】

本発明のオペレータ管理テーブルの構成例を示す図

210

オペレータID	パスワード	アクセスレベル
12345678	AX2BBY3C	特権用
23456789	BY3CCZ4D	一般用
34567890	CZ4DDA5E	デモ用
⋮		

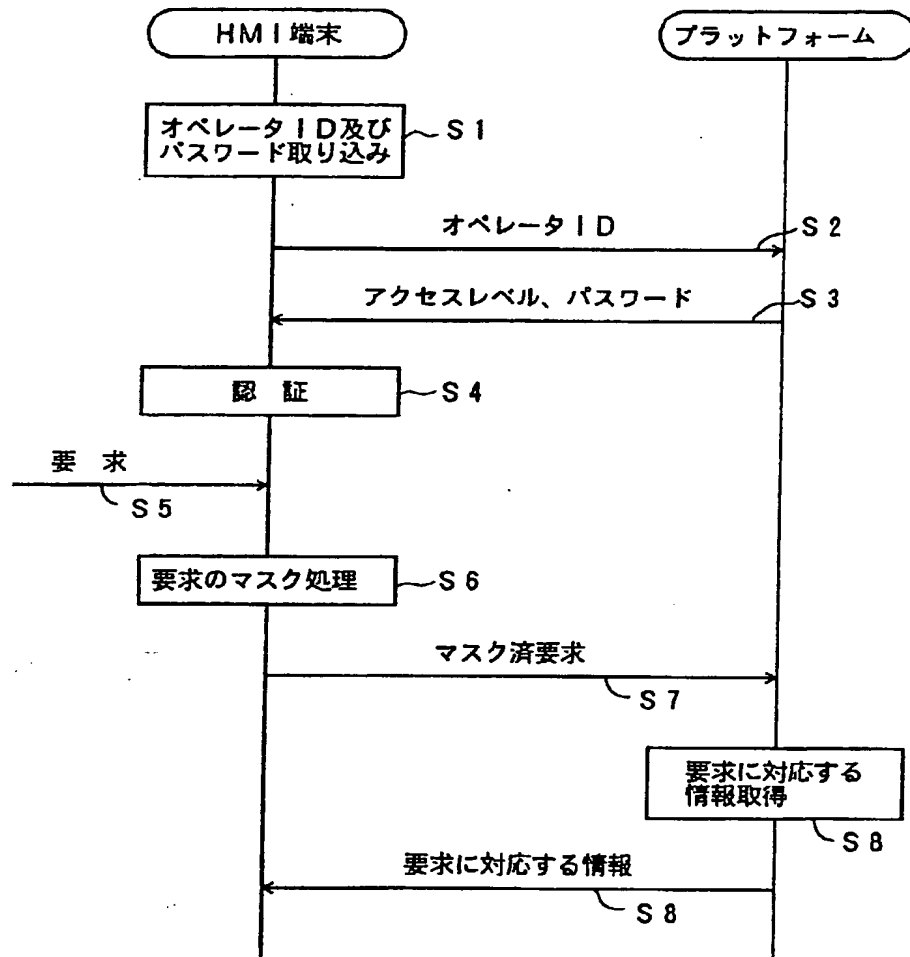
【図10】

本発明の第1の実施例のアクセスレベルとマスクをかけた要求内容の例を示す図

オペレータのアクセスレベル	マスクをかけた要求内容
特 権	実際の苦情の全リストの一覧 (オペレータの要求内容のまま)
一 般	オペレータの担当する苦情の リストの一覧
デ モ	デモ用の苦情のリストの一覧
⋮	

【図1】

本発明の第1の原理を説明するための図



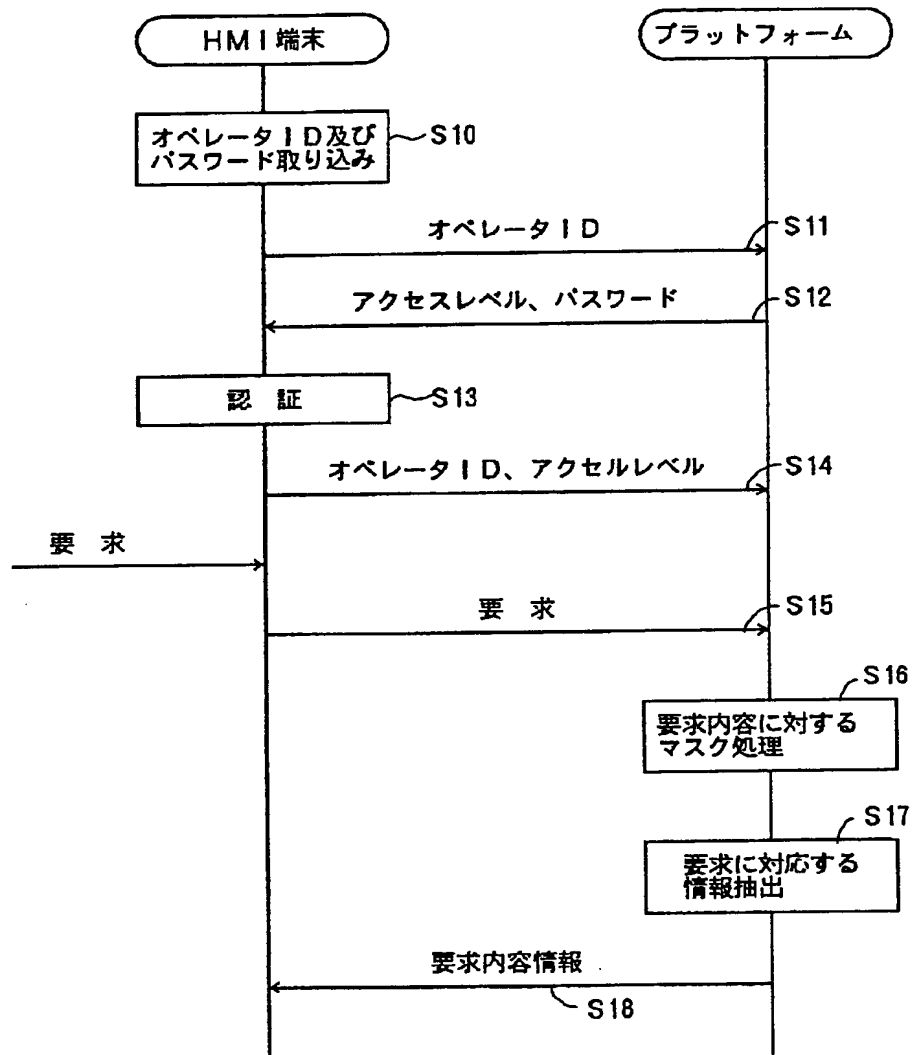
【図12】

本発明の第3の実施例のアクセスレベルと  
マスクをかけた要求内容の例を示す図

オペレータのアクセスレベル	マスクをかけた要求内容
特 権	全ての解約者の情報を消去する
一 般	オペレータが担当した解約者の情報のみを消去する
デ モ	デモ用の解約者の情報を消去する

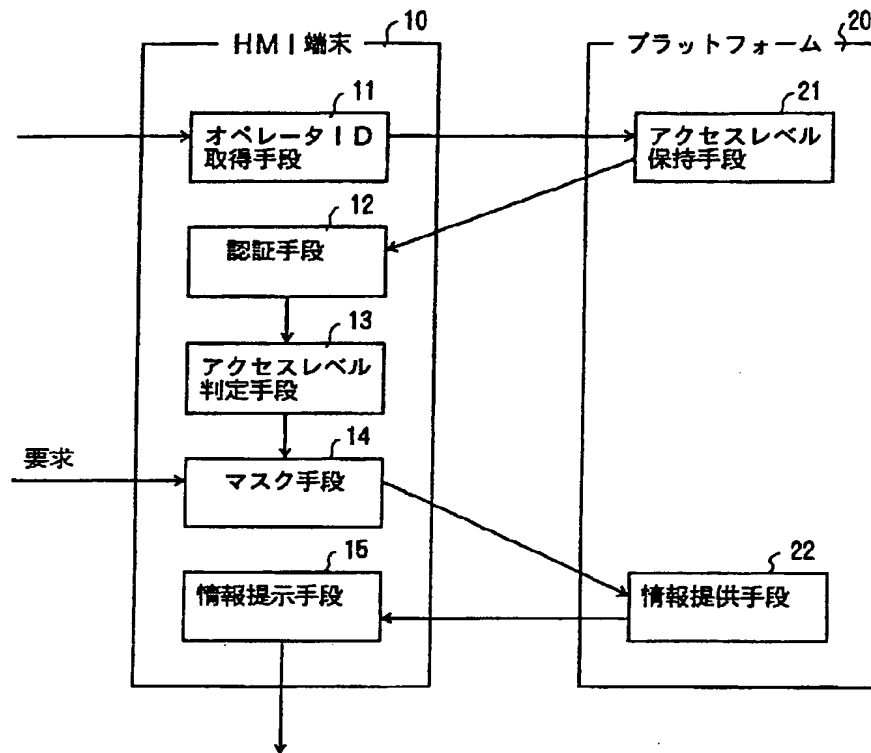
【図2】

本発明の第2の原理を説明するための図



【図 3】

本発明の第 1 の原理構成図



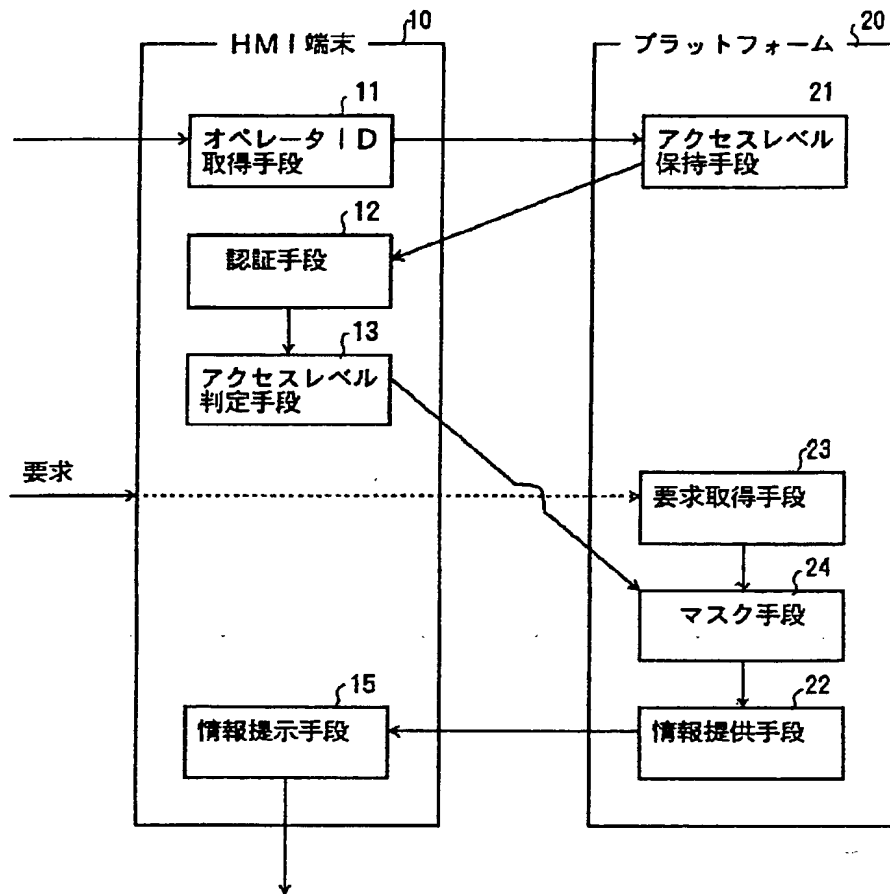
【図 11】

本発明の第 2 の実施例のアクセスレベルと  
マスクをかけた要求内容の例を示す図

オペレータのアクセスレベル	マスクをかけた要求内容
特 権	実際の全顧客の契約条件の一覧 (オペレータの要求内容のまま)
一 般	オペレータの所属する部署の 担当する顧客の契約条件の一覧
デ モ	デモ用の顧客の契約条件の一覧
⋮	

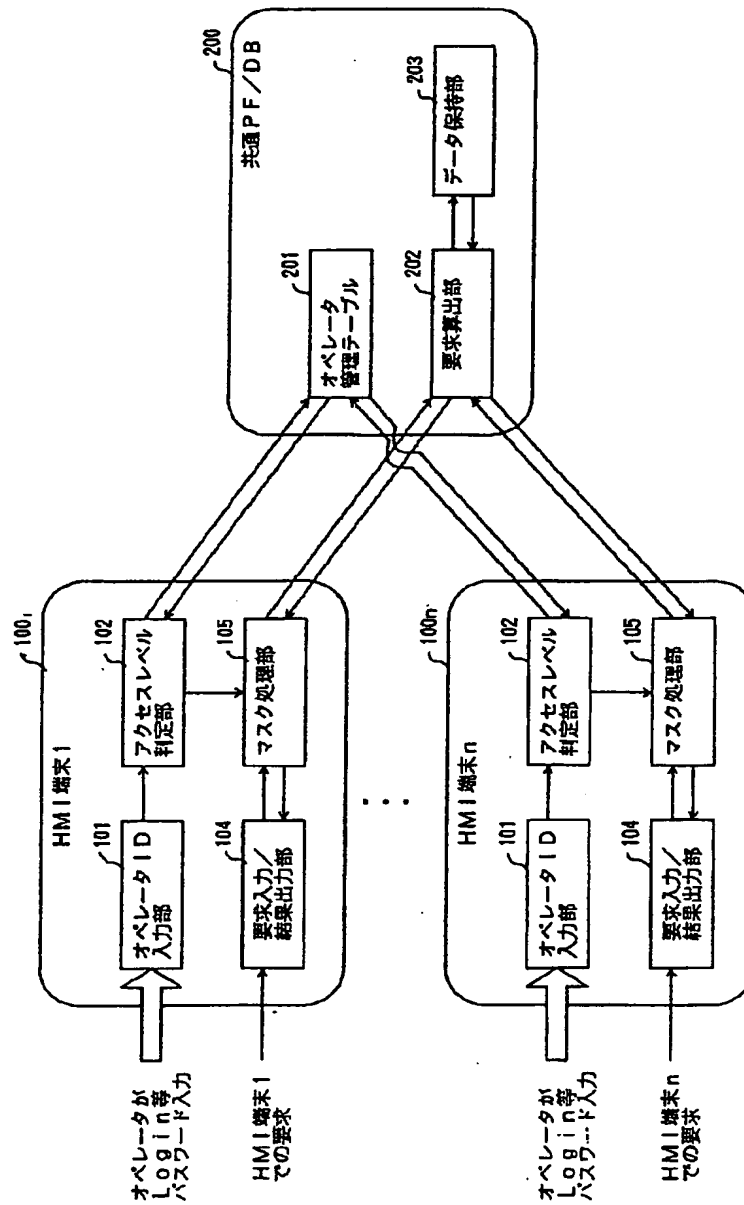
【図4】

本発明の第2の原理構成図



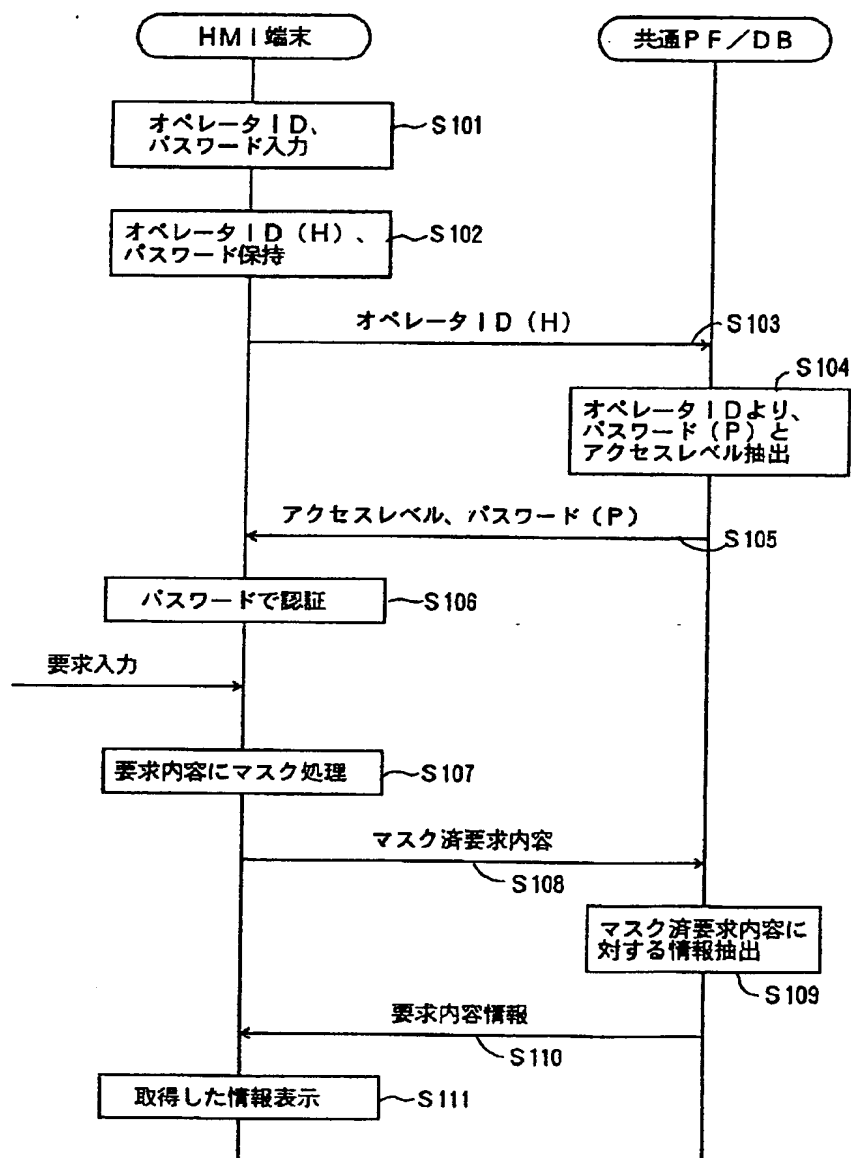
【図5】

本発明の第1のアクセスレベルによるHMI端末の  
利用機能のマスクシステムの構成図



【図7】

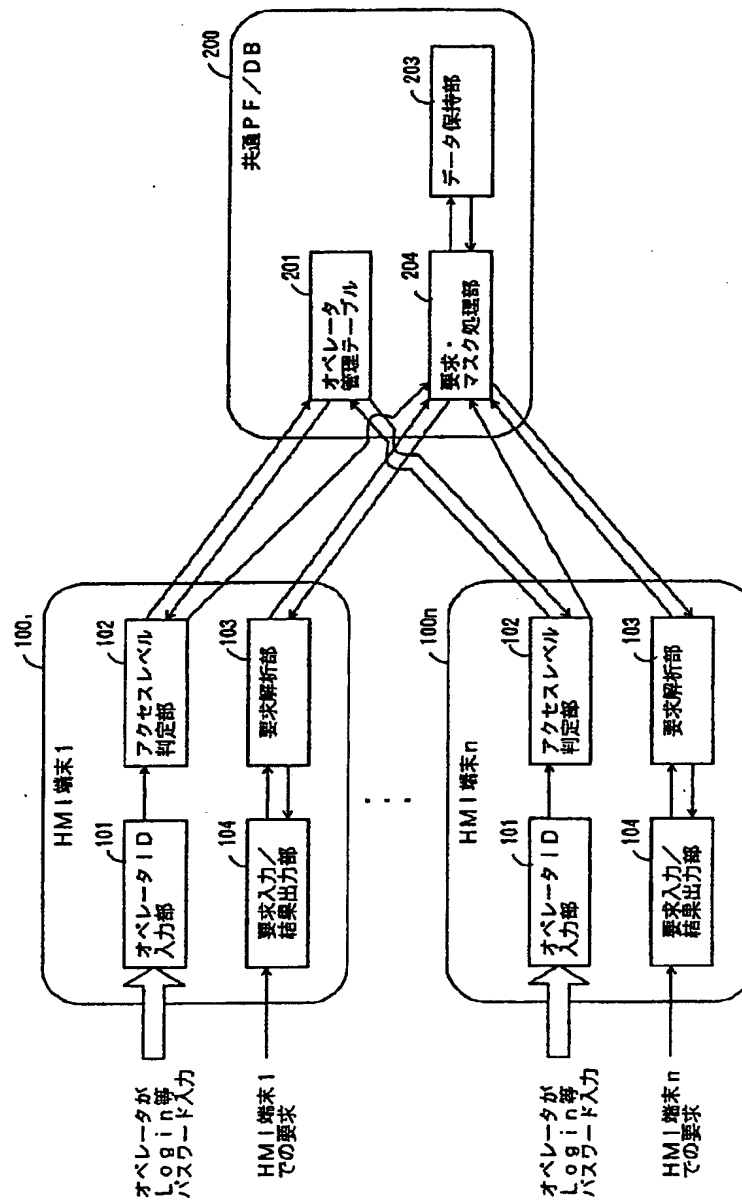
本発明の第1のアクセスレベルによるHMI端末の利用機能の  
マスクシステムの動作を示すシーケンスチャート





【図8】

本発明の第2のアクセスレベルによるHMI端末の  
利用機能のマスクシステムの構成図



【図 9】

本発明の第 2 のアクセスレベルによる HMI 端末の利用機能の  
マスクシステムの動作を示すシーケンスチャート

